JOURNAL OFFICIEL

DU GRAND-DUCHÉ DE LUXEMBOURG

MÉMORIAL A

N° 13 du 3 janvier 2018

Institut Luxembourgeois de Régulation - Règlement ILR/T17/11 du 14 décembre 2017 relatif aux spécifications techniques pour l'interception des communications électroniques au Luxembourg - Secteur communications électroniques.

La Direction de l'Institut Luxembourgeois de Régulation,

Vu la loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques et notamment son article 4 ;

Vu la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et notamment son article 5 ;

Vu la consultation publique nationale du 14 septembre 2017 au 16 octobre 2017 concernant le projet de règlement relatif aux spécifications techniques pour l'interception des communications électroniques au Luxembourg ;

Vu les réponses à la consultation publique susvisée ;

Arrête :

Titre I - Champ d'application et définitions

Art. 1er.

Le présent règlement a pour objectif de définir le format et les modalités de mise à disposition des données techniques et des équipements afin de permettre aux autorités compétentes en la matière l'accomplissement de leurs missions légales de surveillance des communications. Sont notamment visées les mises à disposition de toutes formes de communications interceptées et des données y afférentes en vertu des articles 67-1, 88-1, 88-2 du Code de procédure pénale ainsi que de l'article 7 de loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État (ci-après « la loi du 5 juillet 2016 »).

Art. 2.

Au sens du présent règlement, on entend par :

(1) autorisation : décision prise conformément aux articles 67-1, 88-1 et 88-2 du Code de procédure pénale et 7 de la loi du 5 juillet 2016, et ordonnant une mesure de surveillance ;

(2) autorité légale : les autorités compétentes agissant conformément aux articles 67-1, 88-1 et 88-2 du Code de procédure pénale et agissant dans le cadre de l'article 7 de la loi du 5 juillet 2016 ;

(3) cible : personne physique ou morale à l'encontre de laquelle la mesure de surveillance est ordonnée ;

(4) communication interceptée : communication faite moyennant un réseau ou service de communication électronique et faisant l'objet d'une mesure d'interception ;

(5) mesure d'interception : mesure de surveillance appliquée à l'égard des communications d'une cible aux fins d'accéder à tout contenu, y compris les données afférentes, ainsi qu'à toute information relative aux communications en question ;

(6) mesure de surveillance : mesure ordonnée en application des articles 67-1, 88-1 et 88-2 du Code de procédure pénale ainsi que de l'article 7 de la loi du 5 juillet 2016 ;

(7) exploitant : opérateur ou toute entreprise notifiée conformément à la loi du 27 février 2011 sur les réseaux et les services de communications électroniques ;

(8) service-cible : un réseau de communication public ou un service de communications électroniques visés par une mesure de surveillance.

Titre II - Mise à disposition des communications surveillées

Art. 3.

Dans le respect de l'autorisation légale, la mise à disposition par l'exploitant des données de la mesure d'interception à l'autorité légale concernée, en ce compris la communication interceptée, doit se faire en temps réel. La forme dans laquelle les données doivent être transmises et les modalités techniques de la transmission, sont définies dans les spécifications techniques nationales (National Specifications for Luxembourg) qui se trouvent en annexe du présent règlement et en font partie intégrante.

Art. 4.

Dès la notification de l'autorisation légale à l'exploitant, celui-ci s'efforce à mettre en œuvre incessamment les mesures d'interception ordonnées sans que cette mise en œuvre ne puisse dépasser les délais maxima suivants :

Circonstances	**Délai maximum**
opération de routine l'autorisation légale est notifiée pendant les heures de bureau	4 heures
opération urgente l'autorisation légale est notifiée pendant les heures de bureau	30 minutes
opération urgente l'autorisation légale est notifiée **en dehors** des heures de bureau	2 heures

Art. 5.

(1) Au cas où un exploitant utilise des procédés de codage, de compression ou de chiffrement, les informations interceptées sont à délivrer aux autorités légales en clair.

(2) Au cas où un exploitant modifie le contenu d'une communication, il est également tenu à le reconvertir dans sa forme initiale avant de le transférer à l'autorité légale effectuant la mesure d'interception.

(3) Au cas où la cible modifie le contenu d'une communication par chiffrement ou codage ou en lui administrant tout autre traitement de chiffrement, l'exploitant devra offrir tout le support possible aux autorités légales pour faciliter l'anéantissement de ce genre de chiffrement.

Titre III - Mesures de sécurité

Art. 6.

(1) Le dispositif d'interception de communications ne doit en aucun cas modifier la prestation du service-cible ni fournir une indication à un utilisateur de celui-ci qu'une mesure d'interception est en cours.

(2) L'exploitant doit tenir un registre de toutes activités liées aux mesures d'interception. Ce registre doit contenir les informations suivantes pour chaque opération (initialisation d'une mesure d'interception, prolongation, clôture d'une mesure d'interception, etc.) :

a) l'identité de la personne autorisée ayant effectué l'opération ;
b) référence(s) du service ayant été l'objet de l'opération ;
c) genre d'opération effectuée ;
d) date et heure de l'opération.

(3) Un contrôle du registre par l'autorité légale concernée doit être accordé à tout moment.

(4) L'exploitant est tenu de protéger de façon adéquate les informations relatives aux mesures d'interception et aux équipements utilisés et de ne les divulguer à quiconque d'autre que les personnes autorisées mentionnées ci-dessus sans que l'autorisation écrite ne soit transmise préalablement par l'autorité légale concernée.

(5) Tout accès non-autorisé réel ou tenté pour obtenir des informations sur les mesures d'interception et sur les équipements utilisés est à signaler à l'autorité légale concernée.

Titre IV - Dispositif d'interception

Art. 7.

(1) Le dispositif d'interception utilisé dans le cadre des mesures d'interception doit pouvoir permettre l'interception simultanée d'une même cible par plusieurs autorités légales différentes et ceci pour tous les services-cibles.

(2) Les mesures d'interception des différentes autorités légales doivent rester séparées de façon à éviter que les cibles de l'une des autorités légales ne soient divulguées à une autre.

Art. 8.

La fiabilité et la qualité de service d'un dispositif d'interception doivent au moins être égales à la fiabilité et la qualité de service du service-cible.

Titre V - Dispositions diverses

Art. 9.

(1) À partir de son entrée en vigueur, les exploitants disposent d'un délai de douze mois pour faire les adaptations requises suite à la modification de l'annexe au présent règlement par rapport à l'annexe au règlement 14/184/ILR du 15 décembre 2014 relatif aux spécifications techniques pour l'interception des communications électroniques au Luxembourg.

(2) Une prorogation de douze mois du délai visé au paragraphe (1) peut être accordée par l'Institut pour des services de faible importance sur le marché des communications électroniques. À cette fin, l'exploitant introduit auprès de l'Institut une demande écrite, documentant la faible importance du service visé sur le marché des communications électroniques.

(3) Une prorogation accordée conformément au paragraphe (2) peut être renouvelée à l'issue de douze mois, lorsque les services de communications électroniques concernés sont de moindre importance sur le marché des communications électroniques, lorsque leur importance sur le marché des communications électroniques est en déclin rapide et définitif ou lorsque les équipements respectifs approchent à la fin de leur cycle de vie.

(4) L'importance sur le marché des communications électroniques d'un service, telle que visée aux paragraphes (2) et (3) s'apprécie notamment par le nombre d'utilisateurs, le chiffre d'affaires et la pertinence du service pour les autorités légales.

(5) Avant toute décision d'accorder une prorogation, la demande de l'exploitant est transmise par l'Institut aux autorités légales pour avis. La décision est notifiée par l'Institut au demandeur et aux autorités légales.

Titre VI - Dispositions abrogatoires et finales

Art. 10.

Le règlement 14/184/ILR du 15 décembre 2014 relatif aux spécifications techniques pour l'interception des communications électroniques au Luxembourg est abrogé.

Art. 11.

Le présent règlement sera publié au Journal officiel du Grand-Duché de Luxembourg et sur le site Internet de l'Institut.

La Direction,

Michèle Bram	**Camille Hierzig**	**Luc Tapella**
Directrice adjointe	*Directeur adjoint*	*Directeur*

ANNEXE :

National Specifications for Luxembourg

Table of contents

Introduction

This document consists of Part A and Part B :

PART A : Specification for passive interception
This part describes the technical implementation of lawful interception of telecommunications. Implementation is carried out on the basis of the relevant ETSI specifications (refer to A.1), and this part describes the options and amendments that have been defined for Luxembourg.

PART B : Specification for active interception
This part describes the support that shall be supplied by the NWO/AP/SvP (Network Operator / Access Provider / Service Provider) in case of operations which require active interception.

Scope

This document is written in English and will be provided to the NWO/AP/SvP upon request. It applies to any NWO/AP/SvP in the Grand Duchy of Luxembourg that is obligated to comply in lawful interception.

Part A : Specification for passive interception

Basis of this specification

This Part A includes the ETSI documents listed below, which are applicable in the version noted as follows or in later versions, and are to be observed.

[1] ETSI TS 101 671	**V3.14.1**	**(2016-03) :**	**Lawful Interception (LI) ; Handover Interface for the lawful interception of telecommunications traffic**
[2] ETSI TS 133 108 System	**V14.0.0**	**(2017-04) :**	**Universal Mobile Telecommunications (UMTS) ; LTE ; 3G security ; Handover interface for Lawful Interception (LI)**
[3] ETSI TS 102 232-1	**V3.13.1**	**(2017-03) :**	**Lawful Interception (LI) ; Handover Interface and Service-Specific Details (SSD) for IP delivery ; Part 1 : Handover specification for IP delivery**
[4] ETSI TS 102 232-2	**V3.10.1**	**(2016-08) :**	**Part 2 : Service-specific details for messaging services**
[5] ETSI TS 102 232-3	**V3.5.1**	**(2017-03) :**	**Part 3 : Service-specific details for internet access services**
[6] ETSI TS 102 232-4	**V3.3.1**	**(2017-03) :**	**Part 4 : Service-specific details for Layer 2 services**
[7] ETSI TS 102 232-5	**V3.7.1**	**(2017-03) :**	**Part 5 : Service-specific details for IP Multimedia services**
[8] ETSI TS 102 232-6	**V3.3.1**	**(2014-03) :**	**Part 6 : Service-specific details for PSTN/ ISDN services**
[9] ETSI TS 102 232-7	**V3.4.1**	**(2017-03) :**	**Part 7 : Service-specific details for Mobile Services**

The chosen options and national amendments to these ETSI documents are listed in the following chapters of Part A. If no options or amendments are defined in Part A, the corresponding ETSI document will be applicable without change in the version specified above or in a later version.

List of abbreviations

Abbreviation	Description
3GPP	3rd Generation Partnership Project
AP	Access Provider
ASN.1	Abstract Syntax Notation One
CC	Content of Communication
CCLID	CC Link IDentifier
CSP	Communication Service Provider
CUG	Closed User Group
DSL	Digital Subscriber Line
ETSI	European Telecommunications Standards Institute
FTP	File Transfer Protocol
GGSN	Gateway GPRS Support Node
GLIC	GPRS LI Correlation
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HI 1	Handover Interface 1
HI 2	Handover Interface 2
HI 3	Handover Interface 3
ID	Identifier
IPSec	Internet Protocol Security
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
LALS	Lawful Access Location Services
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LIID	Lawful Interception Identifier
NEID	Network Element Identifier
NID	Network Identifier
NWO	Network Operator
ROSE	Remote Operation Service Element
RTP	Real-Time Transport Protocol
SGSN	Serving GPRS Support Node
SMS	Short Message Service
SSD	Service-Specific Details

SvP	Service Provider
TCP	Transmission Control Protocol
TS	Technical Specification
UDP	User Datagram Protocol
ULIC	UMTS LI Correlation
UMTS	Universal Mobile Telecommunication System
UPS	Uninterruptible power supply
UUS	User to User Signalling
VPN	Virtual Private Network

Chosen options and amendments

Re [1] (TS 101 671)

Options that can be chosen in each country and amendments to [1] are listed in this chapter.

Re [1], General section

Re Section	Reference / Description	National provision / extension
5.1	**Handover interface 1 (HI1)** Design, electronic or manual	The HI1 interface will remain manual. If a legal basis is created for electronic implementation of the HI1 interface, this will be introduced at a later stage. Exception : LI management notifications (LI BEGIN, LI MODIFY, LI END, ALARM) shall be sent via the electronic HI2 interface (refer to [1], D.4).
5.2	**Handover Interface port 2 (HI2)**	The IRI records shall be transmitted individually.
6.1	**Lawful Interception Identifier (LIID)**	The LIID shall be defined by the LEA.
6.2.1	**Network Identifier (NID)**	The NID consists of the Operator ID and Network Element Identifier (NEID). The Operator ID consists of up to 5 characters ; the nomenclature is defined and updated by the LEA. The NEID is 1-25 characters long, as defined in [1] and shall be set by the NWO/AP/SvP.
7.2	**LI notifications towards the LEMF**	LI management notifications (LI BEGIN, LI MODIFY, LI END, ALARM) shall be sent via the electronic HI2 interface (refer to [1], D.4).
8.1	**Data transmission protocols (HI2)**	Only FTP shall be used, ROSE shall not be used.
9	**HI3 : Interface port for Content of Communication**	The Content of Communication (CC) shall be presented as a transparent en clair copy, if the encryption is managed by the network. Encryption not managed by the network, e.g. user provided end-to-end encryption, need not to be removed by the network.
10.1	**Timing**	If IRI cannot be transmitted, they shall be buffered by the NWO/AP/SvP. Minimum buffer time : 3 days
11	**Security aspects**	ISDN transmission : An ISDN CUG (Closed User Group) shall be formed as specified by the LEA. IP-based transmission : A VPN including IPSec encryption will be set up between the NWO/AP/SvPs obliged to provide for intercepts and the LEAs, refer to explanations in chapter A.4 of this document.

Re Section	Reference / Description	National provision / extension
12	**Quantitative aspects**	The following figures can be used as a basis for dimensioning the technical equipment installed at the NWO/AP/SvPs : • 50 targets for the first 10000 subscribers • an additional 20 targets for each further 10000 subscribers started (e.g. : NWO with 76000 subscribers shall be able to set up at least 50+7*20 = 190 targets)

Re [1], Annex A circuit-switched network handover

Re Section	Reference / Description	National provision / Extension
A.1.3	**Use of identifiers**	As option A (A.5.4.1) has been specified in A.5.4, the rules according to table A.1.1, left side, apply.
A.3.2	**Structure of IRI records**	Only IRI conforming to ASN.1 - description are permissible.
A.3.2.1	**Control information for HI2, item 5**	Date and time shall be transmitted as local time.
A.4	**HI3 : Interface port for Content of Communication**	The Content of Communication (CC) shall be presented as a transparent en clair copy, if the encryption is managed by the network. Encryption not managed by the network, e.g. user provided end-to-end encryption, need not be removed by the network.
A.4.1	**Delivery of Content of Communication (CC)**	Use of UUS1 has been specified. In order to enable sub-addressing as fall-back, the LIID for circuit-switched intercepts shall solely be implemented by number (LIID is set by the LEA).
A.4.2	**Delivery of packetized Content of Communication (CC)**	Text messages (SMS) and UUS shall be transmitted via the HI2 interface.
A.4.4.1	**Failure of CC links**	The NWO/AP/SvP shall make 3 attempts at an interval of 5 seconds.
A.4.4.2	**Fault reporting**	Error messages shall be transmitted over HI2 in accordance with Annex D.4, if the system used by the NWO/AP/SvP supports this functionality.

Re Section	Reference / Description	National provision / Extension
A.4.5	**Security requirements at the HI3 interface port**	Refer to 5.1.1, re 11. Security Aspects
A.5.4	**Multi party calls - general principles, options A, B**	Option A shall be used.
A.6.4.1	**Explicit call transfer, CC link**	Option 2 has been specified.
A.6.22	**User-to-User signalling (UUS)**	Transmission via HI2 shall be used, also refer to A.4.2.
A.8.3	**HI3 (delivery of CC)**	Correlation information is transmitted in conformance with 5.1.2, sec. A.4.1.
A.8.4	**HI2 (delivery of IRI)**	Redundant information shall be sent for each further event.

Re [1], Annex C HI2 delivery mechanisms and procedures

Re Section	Reference / Description	National provision / Extension
C	**ROSE or FTP**	Only FTP shall be used, ROSE shall not be used.
C.2.2	**Use of FTP**	Method B shall be used.

Re [1], Annex D Structure of data at the handover interface

Re Section	Reference / Description	National provision / Extension
D	**ASN.1 object tree**	Additional national parameters will be established, refer to Annex A for the definition.

Re [1], Annex E Use of subaddress and calling party number…

Re Section	Reference / Description	National provision / Extension
E.2	**Subaddress options**	According to Table E.2.1 in [1], the default value for type of subaddress is “user specified”.
E.3.2	**Field order and layout**	To distinguish between "old" transmission and transmission in accordance with this specification, the octets 16-23 are allocated as follows : If ‘old’ transmission : no entry If transmitting according to this specification : "Xa.bb.cc" X : E for ETSI a : main version TS 101 671 bb : technical version cc : editorial version (Example : E3.14.01 for TS 101 671 V3.14.1)

Re [1], Annex F GPRS HI3 interface (includes 3GPP as ref. in [1])

Re Section	Reference / Description	National provision / extension
F.1	**Functional architecture**	GGSN and SGSN interception shall be set as standard in order to obtain a maximum of information. If for technical reasons only one kind of interception is possible, then SGSN interception shall be set up.
F.3	**HI3 Delivery of Content of Communication (CC)**	Transmission by GLIC/TCP or FTP/TCP shall be used, GLIC/UDP shall not be used.
F.3.2.2	**Use of FTP**	Method B shall be used.
F.3.2.2	**Use of FTP**	The following triggers have been specified : send timeout = 10s volume trigger = 10 MByte

Re [1], Annex D.5 ASN.1 - description of IRI (HI2)

Clarification : Any parameter described in the ASN.1 notation, even if marked as OPTIONAL in the ETSI TS, SHALL be transmitted, insofar it exists with regard to the respective message.

ASN.1-Reference	Reference / Description	National provision / Extension
04022.1(1)	**Location**	In case of a mobile connection, the following parameters shall be set : - globalCellID - gsmlocation or umtslocation
04022.1	**Location/gsm Location/ GeoCoordinates**	The AZIMUTH value shall be set except in the case of an omni-directional antenna (360° antenna).
04022.1	**National HI2-ASN1parameters/ LuxParameters**	National parameters have been defined in addition to the ASN.1 description in [1] : the description can be found in Annex A.
04022.1	**partyinformation**	An individual partyinformation shall be sent for EACH party involved in a communication.
04022.1	**partyinformation/partyidentity**	All existing parameters shall be defined, depending on the means of communication used.

Re [2] (TS 133 108)

The options that can be chosen in each country and amendments to [2] are listed in this chapter.

Re [2], General section

Re Section	Reference / Description	National provision / Extension
4.4.1	**Handover Interface port 2 (HI2)**	The IRI records shall be transmitted individually.
4.5	**HI2 : Interface port for intercept related information**	If it is not possible to transmit the IRI, they shall be buffered by the NWO/AP/SvP. Minimum buffer time : 3 days
4.5.1	**Data transmission protocols (HI2)**	Only FTP shall be used, ROSE shall not be used.
5.1.2.1	**Network Identifier (NID)**	The NID consists of the Operator ID and Network Element Identifier (NEID). The Operator ID consists of up to 5 characters ; the nomenclature is defined and updated by the LEA. The NEID is 1-25 characters long, as defined in [1] and shall be set by the NWO/AP/SvP.
5.1.5	**Use of identifiers**	As option A (5.4.4.1) has been specified in 5.4.4, the rules according to table 5.1, left side, apply.
5.2.2.1	**Control information for HI2, item 5**	Date and time shall be transmitted as Local Time.
5.2.3	**HI2 (delivery of IRI)**	Redundant information shall be sent for each further event.
5.3.1	**Delivery of Content of Communication (CC)**	Use of UUS1 has been specified. In order to enable sub-addressing as fall-back, the LIID for circuit-switched intercepts shall solely be implemented by number (LIID is set by the LEA).
5.3.3	**Security requirements at the interface port of HI3**	ISDN transmission: An ISDN CUG (Closed User Group) shall be formed as specified by the LEA.
5.4.4.0	**Multi party calls - general principles, options A, B**	Option A shall be used.
5.5.4.1	**Explicit call transfer, CC link**	Option 2 has been specified.
5.5.15	**User-to-User signalling (UUS)**	Transmission via HI2 has been specified.
6.2.1 7.2.1 8.2.1 9.2.1 10.2.1 11.2.1 12.2 13.1.2.1	**Timing**	If IRI cannot be transmitted, they shall be buffered by the NWO/AP/SvP. Minimum buffer time : 3 days

Re Section	Reference / Description	National provision / Extension
14.2.3.1		
6.2.1 7.2.1 10.2.1	**Precision of timestamps**	The timestamps shall have a precision of at least 1 millisecond.
6.3 7.3 8.3 9.3 10.3 11.3 12.3 13.1.3 14.2.4.1	**Security aspects**	IP-based transmission : A VPN including IPSec encryption will be set up between the NWO/AP/SvPs obligated to provide for intercepts and the LEAs, refer to A.4 of this document.
6.4 7.4 8.4 9.4 10.4 11.4 12.4 13.1.4 14.2.5.1	**Quantitative aspects**	The following figures can be used as a basis for dimensioning the technical equipment installed at the NWO/AP/SvPs : • 50 targets for the first 10000 subscribers • an additional 20 targets for each further 10000 subscribers started (e.g. : NWO with 76000 subscribers shall be able to set up at least 50+7*20= 190 targets)
6.5.0	**UMTS data events**	The event “start of interception with mobile station attached” mentioned in Table 6.1 shall generate a Report IRI.
6.5.1.1	**REPORT record information**	All events marked as national option or as dependent on national regulations shall generate a Report IRI.
6.6	**IRI reporting for packet domain at GGSN**	This option does not need to be implemented in Luxembourg.
6.7	**Content of Communication interception for packet domain at GGSN**	The option has been chosen. All target traffic available at the interception node shall be routed to the LEA.
7.5.0	**Location Information**	Location information shall be provided except it is explicitly prohibited by the warrant.
12.5	**IRI for IMS-based VoIP**	The national option has been chosen, LEMF shall be informed about the unavailability of CC.

Re [2], Annex A HI2 delivery mechanisms and procedures

Re Section	Reference / Description	National provision / Extension
A	**ROSE or FTP**	Only FTP shall be used, ROSE shall not be used.
A.2.2	**Use of FTP**	Method B shall be used.
A.2.2	**Use of FTP**	The following triggers have been specified : send timeout = 10s

		volume trigger = 10MByte

Re [2], Annex C UMTS and EPS HI3 interface

Re Section	Reference / Description	National provision / Extension
C	**UMTS and EPS HI3 interfaces ; methods of transmission**	Only ULICv1 via TCP stream shall be used.
C.2.2	**Use of FTP**	Method B shall be used.

Re [2], Annex J Use of subaddress and calling party number…

Re Section	Reference / Description	National provision / Extension
J.2.3.2	**Field order and layout**	To distinguish between "old" transmission and transmission in accordance with this specification, the octets 16-23 are allocated as follows : If 'old' transmission : no entry If transmitting according to this specification : "Xa.bb.cc" X : E for ETSI a : main version TS 101 671 bb : technical version cc : editorial version (Example : E3.14.01 for TS 101 671 V3.14.1)

Re [2], Annex O LALS (Lawful Access Location Services)

Re Section	Reference / Description	National provision / Extension
O	**LALS**	NWO/AP/SvPs shall inform LEA if LALS is supported in NWO/AP/SvPs's network. In this case, LALS shall be activated for specific targets upon LEA's request. The required parameters will be defined by the LEA.

Re [2], Annex B Structure of data at the handover interface

Clarification : Any parameter described in the ASN.1 notation, even if marked as OPTIONAL in the ETSI TS, SHALL be transmitted, insofar it exists with regard to the respective message.

ASN.1 - Reference	Reference / Description	National provision / Extension
04022.49(2)	**Eps-HI3-PS**	To avoid any doubt : The timestamp parameter in the ULIC header shall be provided.

Re [3] (TS 102 232-1)

The options that can be chosen in each country and amendments to [3] are listed in this chapter.

Re [3], General section

Re Section	Reference / Description	National provision / Extension
5.2.3	**Authorization country code**	Specified as "LU".
5.2.4	**Communication identifier**	The Operator ID consists of up to 5 characters ; the nomenclature is defined and updated by the LEA.
5.2.6	**Payload timestamp**	Re Note 2 : The ASN.1 MicroSecond-TimeStamp should be used. Re Note 3 : The timeStampQualifier shall be set.
6.2.3	**Aggregation of payloads**	Combined transmission of IP packets is authorised, but shall not delay transmission for more than 2 seconds.
6.2.4	**Sending a large block of application-level data**	Segmentation is not used.
6.2.5	**Padding data**	Padding is not used.
6.2.6	**Payload Encryption**	Payload encryption is not used.
6.3.1	**General**	TCP/IP socket connections are used.
6.3.2	**Opening and closing connections**	The NWO/AP/SvP shall make 3 connection attempts at an interval of 10 seconds. The socket connection shall be closed by the NWO/AP/SvP after 2 minutes of inactivity.
6.3.4	**Keep-alives**	Using Keep-alives may be used if desired, but use shall be agreed between NWO/AP/SvP and LEA. The preferred method is to close the connection after 2 minutes of inactivity according to 6.3.2. If the LEA requests Keep-alives, the function shall be implemented.
6.3.5	**Option negotiation**	Option negotiation is currently not used, but maybe implemented on LEAs request at a later stage.
6.4.2	**TCP Settings**	The port numbers to be used will be specified by the LEA.
6.4.3	**Acknowledging data**	Option 1 is chosen.
7.2	**Security requirements**	IP-based transmission : A VPN including IPSec encryption shall be set up between the NWO/AP/SvPs and the LEAs; refer to A.4.
7.2.3	**Integrity**	NWO/AP/SvPs shall inform LEA if periodic integrity checks are supported in NWO/AP/SvPs's network. In this case, this shall be

		activated upon LEA's request. The required parameters will be defined by the LEA.

Re [3], Annex D IRI by post and pre-processing HI3 information

Re Section	Reference / Description	National provision / Extension
D.4	**IRI by post and pre-processing HI3 information**	Pre-processing at LEMF to generate IRI is not considered, the IRI shall be generated by post-processing at CSP's domain.

Re [3], Annex F Traffic management of the handover interface

Re Section	Reference / Description	National provision / Extension
F.4	**National considerations**	Filtering at the mediation function should be implemented upon request by the LEA.
F.5.2	**Maximum buffering time**	To protect against loss of data due to equipment or network problems, the buffering time shall be 5 minutes taking into account the maximum bandwidth at the network interface of the delivery function.

Supplements to [3], Annex A ASN.1 syntax trees

Clarification : Any parameter described in the ASN.1 notation, even if marked as OPTIONAL in the ETSI TS, SHALL be transmitted, insofar it exists with regard to the respective message.

ASN.1-Reference	Reference / Description	National Provision / Extension
04022.51(3)	**General**	The provisions in [3] remain unchanged.

Re [4] (TS 102 232 – 2)

Re [4], General Section

Re Section	Reference / Description	National provision / Extension
4.2	**Unified messaging**	Handover of intercepted e-mail shall be according to EmailCC and EmailIRI structures.
7	**E-mail attributes**	All attributes mentioned in 7.1 to 7.10 shall be set.

Supplements to [4], Annex D Messaging ASN.1

Clarification : Any parameter described in the ASN.1 notation, even if marked as OPTIONAL in the ETSI TS, SHALL be transmitted, insofar it exists with regard to the respective message.

ASN.1-Reference	Reference / Description	National Provision / Extension
04022.52(4)	**General**	The provisions in [4] remain unchanged.

Re [5] (TS 102 232 – 3)

Re [5], General Section

Re Section	Reference / Description	National provision / Extension
6.2.2	**Use of location field**	The location parameter shall be set.

Supplements to [5], 8 ASN.1 for IRI and CC

Clarification : Any parameter described in the ASN.1 notation, even if marked as OPTIONAL in the ETSI TS, SHALL be transmitted, insofar it exists with regard to the respective message.

ASN.1-Reference	Reference / Description	National Provision / Extension
04022.53(5)	**General**	The provisions in [5] remain unchanged.

Re [6] (TS 102 232 – 4)

Re [6], General Section

The provisions in the specified documents remain unchanged.

Supplements to [6], 8 ASN.1 for IRI and CC

Clarification : Any parameter described in the ASN.1 notation, even if marked as OPTIONAL in the ETSI TS, SHALL be transmitted, insofar it exists with regard to the respective message.

ASN.1-Reference	Reference / Description	National Provision / Extension
04022.54(6)	**General**	The provisions in [6] remain unchanged.

Re [7] (TS 102 232 – 5)

Re [7], General Section

Re Section	Reference / Description	National provision / Extension
5.2.3	**Location information**	The location information shall be reported.
5.6	**Direction for IMS IRI for Signalling Messages**	The payloadDirection parameter shall be used.
5.7.1	**Direction for SIP sessions**	The sessionDirection parameter shall be used.

Supplements to [7], 7 ASN.1 specification for IRI and CC

Clarification : Any parameter described in the ASN.1 notation, even if marked as OPTIONAL in the ETSI TS, SHALL be transmitted, insofar it exists with regard to the respective message.

ASN.1-Reference	Reference / Description	National Provision / Extension
04022.55(7)	**General**	The provisions in [7] remain unchanged.

Re [8] (TS 102 232 – 6)

Re [8], General Section

REMARK : If the NWO/AP/SvP's equipment supports delivery of CC via dedicated ISDN channels as described and defined in [1], this method shall be used for PSTN/ISDN services described in TS 102 232-6 as well.

If delivery of CC via dedicated ISDN channels is not supported by the NWO/AP/SvP's equipment, the CC delivered via RTP according to [8] shall be coded in G.711.

Re Section	Reference / Description	National provision / Extension
6.3.2	**Supplementary information**	All fields mentioned in the table shall be set.

Supplements to [8], Annex A ASN.1 for IRI and CC

Clarification : Any parameter described in the ASN.1 notation, even if marked as OPTIONAL in the ETSI TS, SHALL be transmitted, insofar it exists with regard to the respective message.

ASN.1-Reference	Reference / Description	National Provision / Extension
04022.56(8)	**General**	The provisions in [8] remain unchanged.

Re [9] (TS 102 232 – 7)

Re [9] ; General Section

The provisions in the specified documents remain unchanged.

Supplements to [9] ; Annex A ASN.1 for IRI and CC

Clarification : Any parameter described in the ASN.1 notation, even if marked as OPTIONAL in the ETSI TS, SHALL be transmitted, insofar it exists with regard to the respective message.

Technical Provisions

ISDN-based transmission

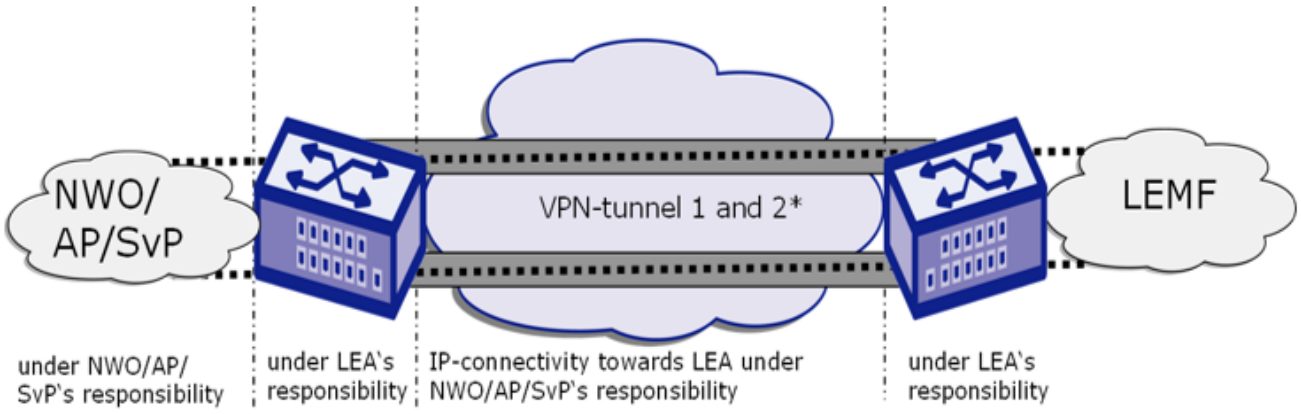
Routing of CC (Content of Communication) is via ISDN dial-up lines using Euro ISDN (E-DSS1). An ISDN CUG (Closed User Group) between the NWO/AP/SvP and the LEA shall be set up.

IP-based transmission

IP-based transmission takes place over a VPN. Provision, configuration and operation of the VPN components are the responsibility of the LEA.

The following components shall be provided by the NWO/AP/SvP :

- Transparent Internet access to each LEA :
  Internet access shall be sized adequately, shall have static, official IP addresses and shall have maximum availability with regard to the infrastructure of the NWO/AP/SvP.
  Internet access needs to be planned and implemented in parallel if required by the LEA for introduction of redundancy. In this case, both Internet accesses should be planned as independently as possible from one another, taking the infrastructure at the NWO/AP/SvP into account (e.g. separate physical entry points, routing, autonomous network components, independent peering points).
- Infrastructure at the handover point :
  The following components are to be supplied by the NWO/AP/SvP :
  - exclusive 19" rack, with lock
  - 2 X 230 VAC, 16 amp. power supply (connected to UPS)
  - waste heat dissipation capacity for the rack : minimum 2kW
  - installation in IT server room
  - transparent Internet access/Internet access terminates in this 19" rack (Ethernet interface)
  - handover from the provider’s network takes place in this 19" rack (Ethernet interface)



* second Internet access upon request by the LEA

Annex A : National HI2-ASN.1 parameters

Additions to HI2-Operations

{itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) hi2(1) version18(18)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS

Natparas FROM NatParameter;

IRI-Parameters ::= SEQUENCE

{
domainID [0] OBJECT IDENTIFIER (hi2OperationId) OPTIONAL,
-- for the sending entity the inclusion of the Object Identifier is mandatory

national-HI2-ASN1parameters[255] National-HI2-ASN1parameters OPTIONAL
}

National-HI2-ASN1parameters ::= SEQUENCE
{
countryCode [1] PrintableString (SIZE (2)),
-- Country Code (LU for Luxembourg) according to ISO 3166-1,
-- the country to which the parameters inserted after the extension marker apply.
-- In case a given country wants to use additional national parameters according to
-- its law, these national parameters should be defined using the ASN.1 syntax and
-- added after the extension marker (...).
-- It is recommended that "version parameter" and "vendor identification parameter"
-- are included in the national parameters definition. Vendor identifications can be
-- retrieved from the IANA web site (see annex H). In addition, avoiding the use
-- of tags from 240 to 255 is recommended in a formal type definition.
natparas [2] Natparas,
-- Import from national specifications for Luxembourg, Annex A
}
END -- HI2Operations

NatParameter

```
-- National parameter
-- Content defined by national law
-- Version of this ASN.1 specification of the national parameters : '1'
-- To be inserted into the parameter "specificationVersion"
-- The coding of all text fields shall be according to CODEPAGE 1252

NatParameter

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

 Natparas ::= SEQUENCE

{
        natVersion              [1]    SEQUENCE

        {
                Version  [1]    INTEGER(0..255)

        },
        locationDetails         [2]    LocationDetails OPTIONAL

}
-- ***************************** Parameter begin **********************
 LocationDetails ::= SEQUENCE

{
        radius                  [0]    INTEGER(0..2147483647) OPTIONAL,
        -- radius of a cell in metres
        radiationDirection      [1]    INTEGER(0..359) OPTIONAL,
        -- radiation direction of the main beam of a cell in degrees relative to true north
        deflectionAngle         [2]    INTEGER(0..360) OPTIONAL,
        -- deflection angle of the cell in degrees
        fieldIntensity          [3]    INTEGER(-200..0) OPTIONAL,
        -- field intensity of the mobile phone in [dbm]
        remark                  [4]    PrintableString (SIZE (256)) OPTIONAL
        -- free text for additional information
        -- (e.g. "antenna position main station, building 16")

}
 -- ***************************** Parameter end **********************

END
```

Specification for active interception

General Requirements

In accordance with the relevant domestic laws, a NWO/AP/SvP shall support the integration of active interception equipment into its network upon request by the LEA.

The active interception equipment will be provided and operated by the LEA responsible.

Depending on the case and the nature of the active interception, the point and type of integration into the NWO/AP/SvP's network and the level of required support may vary.

Prior to the integration, the LEA responsible will communicate the detailed requirements to the NWO/AP/SvP.

Technical Provisions

The required technical provisions will be announced by the LEA on a case-by-case basis. The general infrastructural requirements will be the same as described in chapter A.4.2 of this document.

(1) {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) hi2(1) version18(18)}
(2) {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2) threeGPP(4) hi3eps(9) r12(12) version-0(0)}
(3) {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) li-ps(5) genHeader(1) version24(24)}
(4) {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) li-ps(5) email(2) version16(16)}
(5) {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) li-ps(5) iPAccess(3) version11(11)}
(6) {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) li-ps(5) l2Access(4) version7(7)}
(7) {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) li-ps(5) iPMultimedia(5) version8(8)}
(8) {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) li-ps(5) pstnIsdn(6) version5(5)}